HIPAA Privacy Policies and Procedures
for the
Department for Employee Insurance

PURPOSE:

The Department for Employee Insurance ("DEI") sponsors and administers a group health plan (the Plan) for employees, pursuant to KRS 18A.225, and is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Employees of the DEI's workforce may have access to the individually identifiable health information of Plan participants on behalf of the Plan or on behalf of DEI, for administrative functions of the Plan. HIPAA and its implementing regulations restrict DEI's ability to use and disclose protected health information (PHI). The purpose of the HIPAA Privacy Policies and Procedures for DEI is to ensure DEI's compliance with HIPAA and any applicable regulations. It is DEI's policy to comply fully with HIPAA's requirements. To that end, all DEI's employees and business associates who have access to PHI must comply with these policies and procedures.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by these policies and procedures. DEI reserves the right to amend or change these policies and procedures at any time without notice. To the extent, these policies and procedures establish requirements and obligations above and beyond those required by HIPAA, the policies and procedures shall be objective and shall not be binding upon DEI. These policies and procedures do not address requirements under other federal laws or under state laws.

DEFINITIONS:

Business Associate: "Business associate" means a person who on behalf of DEI, other than a member of DEI's workforce, performs or assists in the performance of the following: (1) claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management or repricing, or (2) any other function or activity regulated by the privacy regulations, or (3) an entity that provides, other than in the capacity as a member of the work force of the covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, or financial services for DEI.

Covered Entity: "Covered entity" means health plans, health care clearinghouses, and health care providers that transmit health information in electronic format and others with respect to ascertaining the compliance of the covered entities and the enforcement of the applicable requirements. For the purpose of these policies and procedures, "covered entity" means DEI.

De-identified protected health information: "De-identified protected health information" means the information that has been de-identified in compliance with HIPAA regulations and for which there is no reasonable basis to believe that it can be used to identify an individual.

Designated Record Set: "Designated record set" is a group of records maintained by or for DEI that includes:

(1) the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or

(2) other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Employee: "Employee" means all members of DEI's workforce such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of DEI pursuant to employment status or contract, whether or not they are paid by DEI. The terms "employee" includes individuals who would be considered part of the workforce under HIPAA.

Employees with Access: "Employees with access" means those employees who have access to protected health information as outlined in Section III of the Policies on Use and Disclosure of PHI.

Health Care Operations: "Health care operations" means any of the following activities to the extent that they are related to Plan administration:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development; and
- business management and general administrative activities.

Payment: "Payment" includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations, including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

Protected Health Information ("PHI"): "Protected health information" or "PHI" means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased. PHI is individually identifiable health information that is (1) transmitted by electronic media, (2) stored or maintained in any electronic media, or (3) transmitted or maintained in any other form or medium.

The terms "use" and "disclosure" are defined as follows:

- *Use.* Use means the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within DEI of DEI, or by a Business Associate of the Plan.
- *Disclosure. Disclosure f*or information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within DEI.

Plan's Responsibilities as Covered Entity

I. Privacy Official and Contact Person

An individual, to be named by the Commissioner of Department for Employee Insurance, will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to these Privacy Policies and Procedures and DEI's notice of Privacy Practices, Business Associate Agreements and Privacy Training. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

II. Workforce Training

The DEI shall train all members of its workforce on its privacy policies and procedures. The Privacy Official is charged with developing training schedules and programs so that all

workforce members receive the training necessary and appropriate to permit them to carry out their functions within Plan. All new employees shall be trained within thirty (30) days of the hire date. After training, all employees shall sign the Department for Employee Insurance Privacy Practice Statement of Understanding.

III. Technical and Physical Safeguards and Firewall

DEI shall, on behalf of the Plan, ensure that the appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets. Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

IV. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Plan;
- the individual's rights; and
- the Plan's legal duties with respect to the PHI.

The privacy notice will inform participants that DEI will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of DEI's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice. The notice of privacy practices will be individually delivered to all participants:

- at the time of an individual's enrollment in the Plan or, in the case of providers, at the time of treatment and consent; and
- within 60 days after a material change to the notice.

The Plan will also provide notice of availability of the privacy notice at least once every three years.

V. Complaints

The Privacy Official will be the Plan's contact person for receiving complaints. The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's

privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy may be imposed against an employee, including but not limited to, termination of employment.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

DEI shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a disclosure of PHI, either by an employee of the Plan an outside consultant/contractor or, business associate that is not in compliance with these policies and procedures, the employee shall immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the participant can be taken.

VIII. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

IX. Plan Document

The Plan document shall include provisions to describe the permitted and required uses and disclosures of PHI by DEI for plan administrative purposes. Specifically, the Plan document shall require DEI to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that any agents, subcontractors, or other business associates to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to DEI;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan;
- report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;

- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures;
- make DEI's internal practices and records relating to the use and disclosure of PHI received from the Plan available to DHHS upon request; and
- if feasible, return or destroy all PHI received from the Plan that DEI still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

The Plan document shall also require DEI to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that DEI agrees to those restrictions; and (2) provide adequate firewalls.

X. Documentation

The Plan's and DEI's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures shall be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures shall be promptly documented. If a change in law impacts the privacy notice, the privacy policy shall be promptly revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice. The Plan and DEI shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Covered entities shall maintain such documentation for at least six years.

Policies on Use and Disclosure of PHI

I. Use and Disclosure Defined

DEI and the Plan will "use and disclose" PHI only as permitted under HIPAA.

II. Workforce Must Comply With DEI's Policy and Procedures

All members of DEI's workforce (described at the beginning of this Policy and referred to herein as "employees") must comply with this Policy and with DEI's, which are set forth in a separate document.

III. Access to PHI Is Limited to Certain Employees

The following employees ("employees with access") have access to PHI:

- Department for Employee Insurance Commissioner's Office;
- Wellness Works Kentucky;
- Member Services Branch;
- Enrollment Information Branch;
- Data Analysis; and
- Financial Management Branch.

The same employees may be named or described in all of these categories. These employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access shall not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy.

IV. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.
PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

V. No Disclosure of PHI for Non-Health Plan Purposes

PHI shall not be used or disclosed for the payment or operations of DEI's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

VI. Mandatory Disclosures of PHI: to Individual and HHS

A participant's PHI shall be disclosed as required by HIPAA in two situations:

• The disclosure is to the individual who is the subject of the information (see policies for "Access to Protected Information and Request for Amendment" that follows); and

• The disclosure is made to HHS for purposes of enforcing of HIPAA.

VII. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. DEI shall describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of DEI's Privacy Official. Uses and disclosures for which no authorization or opportunity to agree or object are required are as follows:

- Uses and disclosures "required by law;"
- Disclosures for public health activities;
- Disclosures regarding victims of abuse and neglect or domestic violence;
- Disclosures for health oversight activities;
- Disclosures for a judicial and administrative proceeding;
- Disclosures for law enforcement purposes;
- Uses and disclosures for cadaveric organ, eye or tissue donation purposes;
- Uses and disclosures for research purposes;
- Uses or disclosure to avert a serious threat to health or safety;
- Uses and disclosures for specialized government functions;
- Uses and disclosures for fundraising; and
- Uses and disclosures for underwriting and related purposes.

VIII. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IX. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. The "minimum-necessary" standard does not apply to any of the following:

• uses or disclosures made to the individual;
• uses or disclosures made pursuant to a valid authorization;
• disclosures made to HHS;
• uses or disclosures required by law; and
• uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making *disclosures* of PHI to business associates for purposes of daily business operations, this is limited to the minimum amount necessary. All other disclosures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making *requests* for disclosure of PHI from DEI for purposes of release of disclosures, only the amount of information reasonably necessary to accomplish the purpose for which the disclosure is requested. All other requests must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

X. Disclosures of PHI to Business Associates

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place.

XI. Disclosures of De-Identified Information

The Plan may freely use and disclose de-identified information. The two ways a covered entity can determine that information is de-identified is as follows: (1) by professional statistical analysis or (2) by removing 18 specific identifiers.

Policies on Individual Rights

I. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- as part of a limited data set;
- for specific national security or law enforcement purposes; or
- disclosures that occurred prior to the compliance date.

The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period. The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure. The first accounting in any 12-month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for subsequent accountings.

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of DEI, the requests are reasonable. However, DEI shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

IV. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is DEI's policy to attempt to honor such requests if, in the sole discretion of DEI, the requests are reasonable. DEI is charged with responsibility for administering requests for restrictions.